(12) UK Patent Application (19) GB (11) 2 333 623 (13) A

(43) Date of A Publication 28.07.1999

(21) Application No 9801441.8

(22) Date of Filing 24.01.1998

(51) INT CL[6]
H04B 1/59

(52) UK CL (Edition Q)
G4H HNNA H13D H14B H14D H14G H60
U1S S2120

(56) Documents Cited
GB 2116808 A EP 0467036 A2 WO 93/25918 A1

(58) Field of Search
UK CL (Edition P) G4H HNEG HNNA , H4L LABA LABB LABX
INT CL[6] G01S

(71) Applicant(s)
GPT Limited
(Incorporated in the United Kingdom)
PO Box 53, New Century Park, Telephone Road, COVENTRY, CV3 1HJ, United Kingdom

(72) Inventor(s)
Neil Andrew McDonald
Melvin Paul Clarkson

(74) Agent and/or Address for Service
GEC Patent Department
Waterhouse Lane, CHELMSFORD, Essex, CM1 2QX, United Kingdom

(54) Abstract Title
Transaction system

(57) A method of operating a transaction system is provided to select one token from a plurality of contactless tokens. A terminal provides power to the tokens by transmission of a radio frequency carrier over an inductive coupling. On receiving a signal from the terminal the tokens generate respective random identifiers. After the tokens have received a command (30) from the terminal, they send return signals (34, 36) to the terminal. Each return signal is sent after a time period which depends on the value of the identifier of that token. When the terminal receives a return signal, it immediately sends an interrupt signal to the tokens which de-activates those which have not yet sent a return signal. Selection continues from among those tokens which did send return signals.

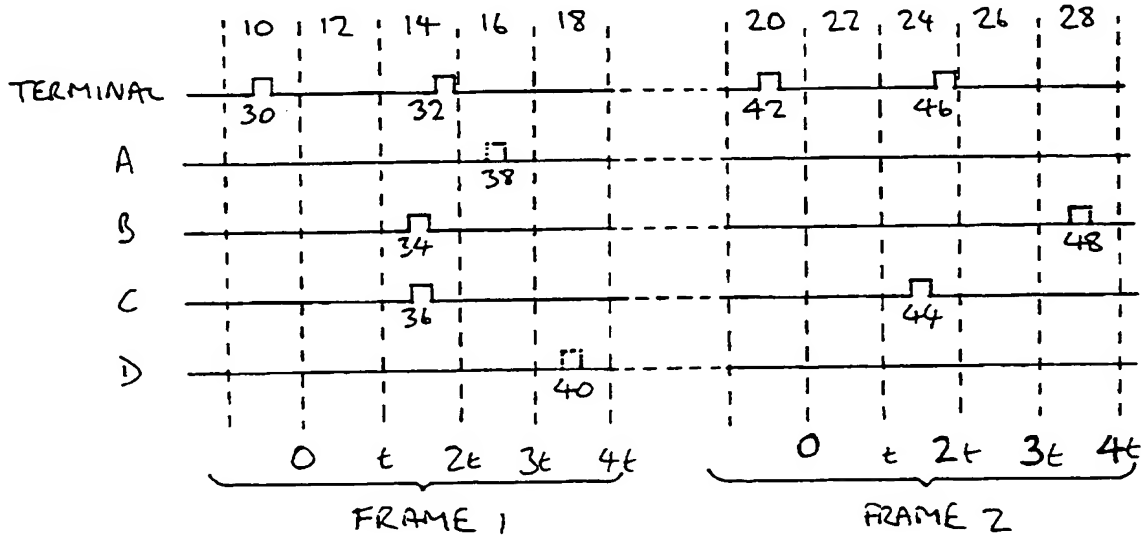

FIG. 1.

GB 2 333 623 A

BNSDOCID: <GB_____2333623A__I_>

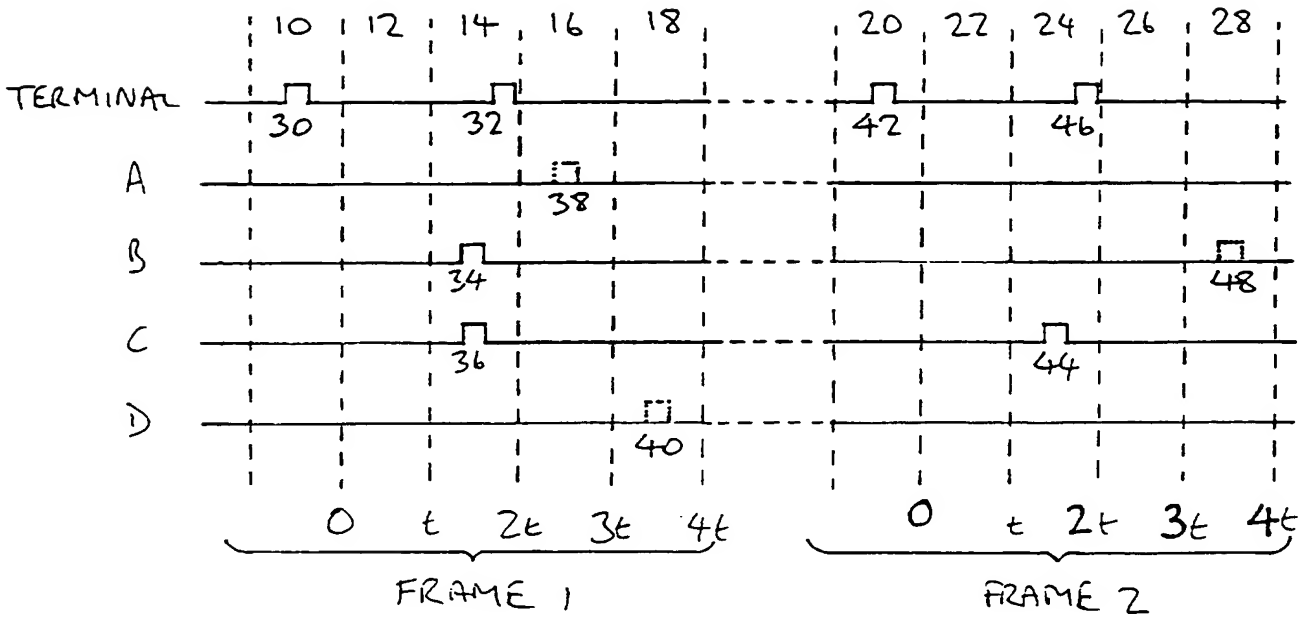

FIG. 1.

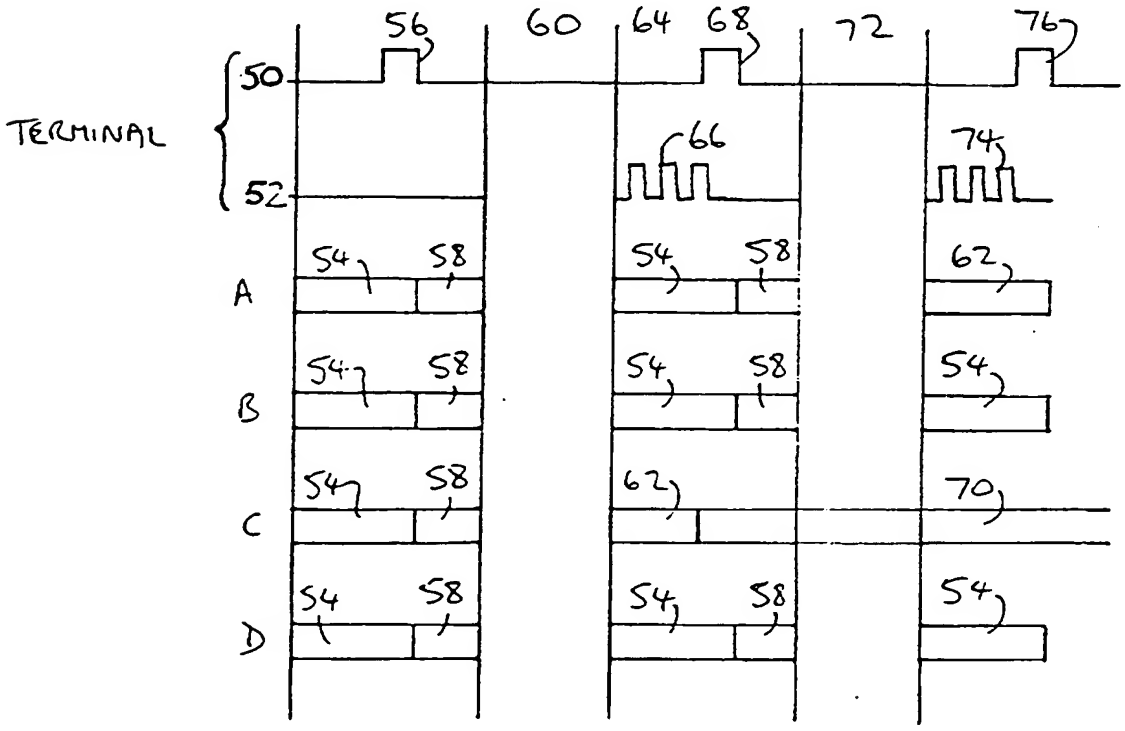

FIG. 2.

BNSDOCID: <GB_____2333623A__I_>

2333623

TRANSACTION SYSTEM

This invention relates to a transaction system in which a portable token, for example a card, is used in conjunction with a device, often termed a terminal, to perform a transaction of some kind. The invention is particularly, but not exclusively, related to smart cards.

Contactless tokens work on, or close to, a terminal which provides power. This power is supplied via a RF (radio frequency) induction field which is referred to as a carrier. Transfer of power from the terminal to the token is akin to the terminal being a primary coil of a transformer and the token a secondary coil. In particular embodiments both the terminal and the token typically each have a single coil aerial

As well as power being transmitted from the terminal to the token, data is transmitted from the terminal to the token and vice versa. The exchange of data is used to perform a transaction. Transmission of data from the terminal occurs by modulating it onto the carrier. Transmission of data from the token to the terminal may be effected by switching an impedance in the token to modulate the amplitude of the carrier at the terminal as the token draws extra power from the terminal due to the switching.

As technology improves, the power consumption of tokens is being reduced. This means that tokens can work further away from the terminal, that is the volume or field of operation of the terminal is larger. If the terminal maintains a fixed power output, it means more tokens can be powered in the field of operation at the same time. Therefore

BNSDOCID: <GB_____2333623A__I_>

the probability of there being more than one token in the field of operation of the terminal is greater.

There can be difficulties in the terminal communicating with a specific token in that signals from the terminal may be picked up by more than one token and that more than one token may reply at substantially the same time. These difficulties could be alleviated or solved by reducing the power output of the terminal which would allow only one token to work within its field of operation. However, this would also reduce the field of operation of the terminal which is a disadvantage from an operational point of view.

A system could be configured such that tokens could be entered into the field of operation of the terminal one at a time. This would allow the terminal to interrogate a single token for its identity. At any stage the terminal could use a list of stored identification numbers to enquire whether a particular token was still in the field of operation. This would be inefficient because it would reduce the amount of time available for the transaction to take place. The terminal could then ask if there was a new token in the field of operation after asking all known tokens to be quiet. This would also be inefficient because the terminal would have to keep repeating this task quickly enough so as not to allow two tokens to enter the field of operation at the same time. Furthermore if two tokens were to enter the field at the same time it is undesirable to request that the user of one of the tokens remove it from the field of operation and then re-enter it simply because the terminal is confused about the tokens

BNSDOCID: <GB_____2333623A__I_>

present in its field of operation. This is because the user may not carry out the request either by accident or intentionally. For example, a token could be left intentionally in the field of operation to defraud the system or to prevent the system from working.

According to a first aspect the invention provides a transaction system comprising a terminal and a plurality of tokens the terminal providing power to the tokens by a carrier transmitted over an inductive coupling characterised in that the tokens each comprise identifier generation means to generate a random identifier and at least one of the tokens sends a return signal to the terminal in response to receiving an outgoing signal sent by the terminal the return signal being sent after a time period which depends on the value of the random identifier.

According to a second aspect the invention provides a method of operating a transaction system to enable a terminal to select one token from a plurality of tokens the terminal providing power to the tokens by a carrier transmitted over an inductive coupling characterised in that the tokens generate random identifiers the terminal sends an outgoing signal to the tokens and at least one of the tokens sends a return signal after a time period which depends on the value of the identifier.

This invention removes the reliance on a unique identifier and so allows a more transparent contactless interface. Therefore it enables existing controllers and their operating systems to be used in their present configurations without modification.

BNSDOCID: <GB_____2333623A__I_>

Preferably the terminal uses a carrier to transmit power to the plurality of tokens.

Preferably the outgoing signal and the return signal occur within a time frame during a selection procedure or event. The selection procedure may be a plurality of steps involved in selecting a single token from the plurality of tokens. Preferably there are a plurality of time frames in the selection procedure. Most preferably there are eight time frames. Preferably there are a plurality of time slots within each time frame.

Preferably the terminal has a field of operation and the tokens are present in the field of operation. Of course, if it so happens that there is only one token present in the field of operation, then the method will not, in this case, be selecting one token from a plurality but will only identify the single token.

Preferably the random identifier is a whole number, that is in the range 0 to n. Conveniently the random identifier is stored in the token in binary form.

Preferably a return signal is sent by the token or tokens having the lowest value of random identifier. If a plurality of tokens have identical random identifiers of lowest value the return signal will be sent at the same time by all of these tokens. The return signals for random identifiers having different values may occur after different time periods following sending of the outgoing signal. Of course, the return signal or return signals could be sent by the tokens having the highest value of random identifier.

BNSDOCID: <GB_____2333823A__I_>

Preferably once the terminal has received at least one return signal from one or more tokens it sends an interrupt signal which is received by all tokens. The interrupt signal prevents the remaining tokens (those that have not sent a return signal) from sending one or more return signals. Conveniently the interrupt signal may be the same as the outgoing signal. Preferably the same interrupt signal that prevents remaining tokens from sending a return signal in a particular time frame is also used to start the next time frame for those tokens which have sent a return signal. In this embodiment the interrupt signal is the next outgoing signal from the terminal. The outgoing signal or the interrupt signal or both may be modulated on the carrier.

Preferably a token takes no further part in subsequent time frames of a selection procedure once it has been prevented from sending a return signal by an interrupt signal.

Preferably the terminal also sends a warm reset signal to all of the tokens present in the field of operation. Conveniently the warm reset is an interruption, that is a temporary stoppage, of information on the carrier without stopping transmission of the carrier itself. Preferably the carrier is modulated with the information. The information may be transaction data or instructions or both. Preferably the information is a continuous tone. The tone may be present on the carrier to be used by each token to derive a clock for its operation.

Preferably the warm reset signal is used by the terminal to inform all tokens that the selection procedure is starting. Conveniently the warm reset allows tokens previously

BNSDOCID: <GB_____2333623A__I_>

prevented from participating further in an earlier selection procedure to participate in a subsequent selection procedure. Preferably the warm reset instructs a previously selected token to become inactive and not participate in the subsequent selection procedure unless otherwise instructed.

Preferably the terminal also sends a cold reset signal to all of the tokens present in the field of operation. Conveniently the cold reset is an interruption, that is a temporary stoppage, of power. This may be done by stopping transmission of the carrier. A cold reset may occur by removing the token away from the field of operation of the terminal and then replacing it. Alternatively a cold reset may occur by keeping the token present near the terminal but interrupting the carrier transmitted by the reader. The former depends on the token user, the latter on the terminal.

Preferably the tokens operate in a contactless manner. They may be contactless smart cards. Preferably the tokens are be powered by an electrical power source such as an RF field. Alternatively they may be powered by an internal power source such as a battery.

Preferably power is sent by the terminal to each token and data is sent by each token to the terminal over a common inductive coupling. This may be provided by the terminal and the tokens each having a single inductive coil.

Preferably the tokens contain hardware logic capable of implementing the method.

Alternatively the tokens contain software capable of implementing the method.

An embodiment of the invention will now be described, by way of example only, with reference to the accompanying figure in which:

Figure 1 shows a selection procedure comprising a series of communication signals between a terminal and a number of tokens; and

Figure 2 shows the effect of the communication signals on the tokens.

In a transaction system comprising a terminal and a plurality of smart cards which transact with the terminal, it is possible that two or more cards will enter the field of operation of the terminal at the same time. This can occur if a person is carrying two contactless cards of the same type in his wallet and waves his wallet near the terminal. In this event either of the cards could power-up first. Therefore if there are two or more cards in the field of operation of the terminal at the same time the terminal needs to identify the cards in order to transact only with one card at one time. It should be noted that once a card has been identified then it is a simple matter to address commands only to that card, for example by appending the identification number of the card to the command in question.

The method described with reference to Figure 1 relates to communication between a terminal and four contactless tokens A, B, C and D. Figure 1 shows a selection procedure comprising two time frames 1 and 2. Communication signals issued by the terminal and each of the tokens are shown occurring during time slots 10, 12, 14, 16, 18,

BNSDOCID: <GB_____2333623A__I_>

20, 22, 24, 26 and 28. Time slot 10 occurs first and time slot 28 occurs last. Time frame 1 comprises time slots 10 to 18 and time frame 2 comprises time slots 20 to 28. It should be noted that although time frame 1 and time frame 2 are shown as distinct and sequential in certain embodiments, they can overlap as will be made clear in the following description.

Before the selection procedure begins, the terminal may send a warm reset to all of the tokens which initiates a time period in which they are made ready for selection.

Referring now to time frame 1, in time slot 10, the terminal first sends a command 30 to all the tokens in its field of operation to instruct them that a selection procedure has started. Although the command 30 may be a warm reset it is preferred that it is one or more data bits. As all of the tokens are in the field of operation of the terminal, they will all receive command 30 at substantially the same time. The rule for the terminal is to send a command to start a time frame. If a return signal from a token is received within the time frame an interrupt signal is immediately sent to end the time frame. There should be as many time frames as is dictated by the laws of probability for there to be a high chance of only one card being selected. If no return signal is received by the end of the time frame there are no selectable tokens in the field of operation, that is there are no tokens in the field of operation or tokens which are present have previously been inactivated.

Each token is provided with a random number generator. This can be in the form of a

BNSDOCID: <GB_____2333623A__I_>

fast oscillator connected to a counter. The frequency of the fast oscillator is made to be heavily dependent on the temperature of the silicon die (-40°C to +125°C) or an unregulated rectified voltage (V_{unreg} in the range 0 to 18V) received by each token from the carrier of the terminal or on both. Since there will be a degree of variation in temperature and V_{unreg} from token to token the frequency of the fast oscillators will also vary from card to card.

The output of the counter connected to the oscillator is latched so as to generate a random number n which can have four values such as 0, 1, 2, 3. When the tokens receive command 30 the counter of each token generates one of the four random values. Each token is configured so as to send a return signal to the terminal after a time period following from command 30 in which the time period is dependent upon the random value n. Referring to Figure 1 it can be seen that each time slot is of duration t μs and so in an individual time frame it is possible that the token can respond in time intervals 0 to t, t to 2t, 2t to 3t or 3t to 4t.

On receiving command 30, the tokens each inspect their random value. A random value of 0 corresponds to a token sending a return signal in slot 12, value 1 corresponds to time slot 14, value 2 corresponds to time slot 16 and value 3 corresponds to time slot 18. The time intervals are directly calculated from a clock generated on each token, which may be directly dependent either upon the frequency of the carrier or on the frequency of a tone which is amplitude modulated onto the carrier. Each token receives the same clock frequency and so can respond in its appropriate time slot. Alternatively

BNSDOCID: <GB_____2333623A_I_>

the token may have an accurate internal time source such as one which is crystal based.

If a token receives an interrupt signal 32 or 46 from the terminal before it has sent its own return signal, it stops transmitting and does not communicate, remaining silent unless it receives a command such as a warm reset from the terminal to start the selection procedure again. The rule for the tokens is to send a return signal in the appropriate time slot unless an interrupt signal is received from the terminal before the return signal is sent. In this event no return signal is to be sent in that selection procedure, that is the token is not to send a return signal in subsequent time frames of that selection procedure. The interrupt signal does not involve an interruption of tone or power being sent to the tokens. Once switched off by the interrupt signal the tokens may not be activated again until they undergo a warm reset.

In the example shown in Figure 1, in time frame 1 tokens A, B, C and D have generated individual random values of 2, 1, 1 and 3 respectively after receiving command 30. Therefore, following command 30 from the terminal none of the tokens respond in time slot 12. In time slot 14 tokens B and C respond with return signals 34 and 36. Accordingly the terminal sends interrupt signal 32 to all of the tokens. Since tokens A and D have random values of higher values than those of B and C , A and D receive the interrupt signal 32 before they have the opportunity to send their return signals. This causes tokens A and D to enter into a waiting state. Therefore the hypothetical occurrences of return signals 38 and 40 from these tokens are only shown with dotted lines. This is the end of theoretical time frame 1. Tokens A and D take no further part

BNSDOCID: <GB_____2333623A__I_>

in this particular selection procedure and they remain in the waiting state until they receive a reset, either a warm reset at the beginning of a subsequent selection procedure or a cold reset.

Time frame 2 now begins. Tokens B and C have both replied and so the terminal knows that there are tokens in its field to be selected. The terminal signals a new time frame to begin by sending a command 42 in time slot 20 to those tokens in its field of operation which are activated and ready to receive further signals, that is tokens B and C. The new command 42 causes tokens B and C to generate new random values. Token B generates a new random value 3 and token C again generates the random value 1. Therefore token C responds with return signal 44 in time slot 24 and the return signal 48 from token B is interrupted and prevented by token B receiving an interrupt signal 46 sent by the terminal.

Of course, to save time, time slots 16 and 18 can be omitted and command 42 would occur in the time slot immediately following time slot 14. To save even more time the interrupt signal 32 and the command 42 can be amalgamated into the same time slot. They could even be the same signal with interrupt signal 32 serving as the new command beginning time frame 2 in which the remaining activated tokens generate new random values and continue the selection procedure.

Although only two time frames are shown in the selection procedure of Figure 1, typically the terminal performs eight time frames in a selection procedure if any return

BNSDOCID: <GB_____2333623A__I_>

signal is received during the first time frame. If there is only one token in the field of operation then eight time frames is simply an overhead. If there are a number of tokens present, for example ten, the likelihood of the selection procedure selecting an individual token is very high (9,999 in 10,000). After eight time frames it is not guaranteed that only one token has been selected. However, this is so likely that the terminal can simply address any activated token and begin a transaction with it. In the rare event that more than one token has been selected after eight frames, the transaction system, or more especially the terminal, can detect the error using check sums or parity checks and can restart the selection procedure.

The selection procedure is terminated if no response is received once time slot 18 has expired because this means that there are no tokens (or no active tokens) in the field of the terminal or the tokens or tokens which were involved in the selection procedure have been removed from the field of operation.

A repetition of the selection procedure a number of times means that each token can be selected in turn and a transaction can be conducted with each.

Figure 2 shows the effect of the communication signals 50 and 52 from the terminal on the state of the tokens A, B, C and D during a number of selection procedures. Communication signals 50 are reset signals and communication signals 52 are transaction data. The transaction data includes commands and interrupt signals such as signals 30, 32, 42 and 46 discussed in relation to Figure 1.

BNSDOCID: <GB_____2333623A__I_>

A token can be in one of several states. A waiting state 54 is achieved after a token has received an interrupt signal from the terminal or undergone a cold reset (not shown). A warm reset 56 causes those tokens in the waiting state 54 to change to a ready state 58, that is to be prepared for a selection procedure which occurs during a time period 60. Time period 60 corresponds to a selection procedure such as that described in relation to Figure 1. Once a token has been selected it is in a selected state 62.

If a token enters the field of operation after the warm reset 56, then the warm reset 56 is not received by the token and therefore it will remain in the waiting state 54. Therefore it will not take part in the selection procedure, such as that indicated by numeral 60 or shown in Figure 1. This is because the token is not in the ready state 58.

Whilst the selection procedure 60 is occurring the tokens will periodically receive command signals from the terminal during individual time frames. If a token is still in a ready state 58 and does not receive a command or interrupt signal in a time interval longer than a time frame, say in a time interval of 0 to 5t, this means that the terminal has stopped carrying out its allocated numbers of time frames within the selection procedure 60. This means that that token is selected and is to become involved in a transaction with the terminal.

This is shown in time period 64 in Figure 2. The terminal now sends transaction data 66 to token C which is now in a selected state 62. This data will be ignored by the other tokens present because they received interrupt signals in selection procedure 60 and are

BNSDOCID: <GB_____2333623A__I_>

in waiting states 54.

Once the terminal finishes its transaction with token C it issues a warm reset 68. This puts token C into a halted state 70 so that it will take no further part in any selection procedure until it has received a cold reset causing it to go back to a waiting state 54.

The same warm reset 68 puts the remaining tokens A, B and D into ready states 58 for a new selection procedure which occurs during time period 72. Only tokens A, B and D take part in this new selection procedure (time period 72). In the example shown, at the end of selection procedure 72 token A has been randomly selected and tokens B and D go back into waiting states 54. The terminal now sends transaction data 74 to token A. A further warm reset 76 continues the sequence. This sequence of selection procedures can be repeated so that all tokens have been selected in turn and then transacted with. The order of selection is random. Once the terminal has selected a token, it can conduct a transaction with it or halt it immediately. The purpose of halting a token immediately is either simply to sense that at least one token is present or to count the number of tokens present by selecting and halting all the tokens until no more can be selected. This enables the terminal to select suitable operating parameters for conducting transactions with the, now known, number of tokens present.

The method works with any number of tokens as long as there is sufficient power from the terminal to energise them all.

BNSDOCID: <GB_____2333623A__I_>

In the example shown the logic is based upon the generation of random numbers 0, 1, 2, 3. Of course, it could be based on any four distinct values or identifiers.

In one embodiment the token and the terminal can both send signals with the same time slot, for example the terminal communicates in the first half of the time slot and the token communicates in the second half of the time slot. If the token generates zero as its random number, it sends a return signal in the same time slot as the terminal sends a command.

A time slot in the selection procedure has a duration typically of 38μs. A time frame on average has a duration typically of two and a half time slots (that is the average value of the random value (0+1+2+3)/4 added to an additional period of time (one time slot) for the terminal to issue commands or interrupt signals or both). This value is calculated assuming that a time frame terminates and a subsequent time frame begins when an interrupt signal is sent by the terminal. If a selection procedure is configured to contain eight time frames, then typically it has a duration of 8 x 2.5 x 38 = 760μs. With overheads the total time required to select a token is less than one millisecond.

It should be noted that the signals sent by the terminal and the token may not be single pulses (although this is simplest) but may be a sequence of pulses so as to reduce the possibility of noise interfering with operation of the method.

This invention can be used with smart cards that do not have a unique identification

BNSDOCID: <GB_____2333623A__I_>

number stored in their memory.

All the functionality described could be implemented either as hardware logic in an ASIC or as software in a token microcontroller.

CLAIMS

1. A transaction system comprising a terminal and a plurality of tokens the terminal providing power to the tokens by a carrier transmitted over an inductive coupling characterised in that the tokens each comprise identifier generation means to generate a random identifier and at least one of the tokens sends a return signal to the terminal in response to receiving an outgoing signal sent by the terminal the return signal being sent after a time period which depends on the value of the random identifier.

2. A transaction system according to claim 1 in which the outgoing signal and the return signal occur within a time frame during a selection procedure or event.

3. A transaction system according to claim 2 in which the selection procedure is a plurality of steps involved in selecting a single token from the plurality of tokens.

4. A transaction system according to claim 2 or claim 3 in which there are eight time frames in the selection procedure.

5. A transaction system according to any preceding claim in which the random identifier is a whole number, that is in the range 0 to n.

6. A transaction system according to any preceding claim in which a return signal is sent by the token or tokens having the lowest value of random identifier.

7. A transaction system according to any preceding claim in which the terminal sends an interrupt signal once it has received at least one return signal from one or more tokens which is received by all tokens.

8. A transaction system according to claim 7 in which a token takes no further part in subsequent time frames of a selection procedure once it has been prevented from sending a return signal by an interrupt signal.

9. A transaction system according to any preceding claim in which a terminal sends a warm reset signal to all of the tokens present in the field of operation to inform them that the selection procedure is starting.

10. A transaction system according to claim 9 in which the warm reset allows tokens previously prevented from participating further in an earlier selection procedure to participate in a subsequent selection procedure.

11. A transaction system according to claim 9 or claim 10 in which the warm reset instructs a previously selected token to become inactive and not participate in the subsequent selection procedure unless otherwise instructed.

BNSDOCID: <GB_____2333623A__I_>

12. A transaction system according to any preceding claim in which the terminal sends a cold reset signal to all of the tokens present in the field of operation.

13. A transaction system according to any preceding claim which comprises contactless tokens.

14. A transaction system according to claim 13 which comprises contactless smart cards.

15. A transaction system according to any preceding claim in which power is sent by the terminal to each token and data is sent by each token to the terminal over a common inductive coupling.

16. A transaction system according to any preceding claim in which the terminal and the tokens each have a single inductive coil.

17. A transaction system substantially as described herein with reference to Figures 1 and 2 of the accompanying drawings.

18. A method of operating a transaction system to enable a terminal to select one token from a plurality of tokens the terminal providing power to the tokens by a carrier transmitted over an inductive coupling characterised in that the tokens generate random identifiers the terminal sends an outgoing signal to the tokens

and at least one of the tokens sends a return signal after a time period which depends on the value of the identifier.

19. A method substantially as described herein with reference to Figures 1 and 2 of the accompanying drawings.

20. A terminal which uses the method of claim 18 or claim 19.

21. A terminal substantially as described herein with reference to Figures 1 and 2 of the accompanying drawings.

BNSDOCID: <GB_____2333623A__I_>

The Patent Office

21

Application No:	GB 9801441.8	**Examiner:**	Mike Davis
Claims searched:	1-21	**Date of search:**	18 March 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4H (HNNA,HNEG), H4L (LABA,LABB,LABX)

Int Cl (Ed.6): G01S

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2116808 A	(SENSORMATIC ELECTRONICS)	1,18 at least
X	EP 0467036 A2	(SAVI TECHNOLOGY)	"
X	WO 93/25918 A1	(SAAB-SCANIA)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB_____2333623A__I_>